FINITE SUBGROUPS OF $\mathbf{PGL_2}(\boldsymbol{K})$

ARNAUD BEAUVILLE

Abstract. We classify, up to conjugacy, the finite subgroups of $\mathrm{PGL}_2(K)$ of order prime to $\mathrm{char}(K)$.

Introduction

The aim of this note is to describe, up to conjugacy, the finite subgroups of $\mathrm{PGL}_2(K)$, for an arbitrary field K. Throughout the paper, *we consider only subgroups whose order is prime to the characteristic of* K.

When $K = \mathbf{C}$, or more generally when K is algebraically closed, the answer is well known: any such group is isomorphic to $\mathbf{Z}/r$, D_r (the dihedral group), $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$, and there is only one conjugacy class for each of these groups. If K is arbitrary, the group $\mathrm{PGL}_2(K)$ is contained in $\mathrm{PGL}_2(\overline{K})$, so the subgroups of $\mathrm{PGL}_2(K)$ are among the previous list; it is not difficult to decide which subgroups occur for a given field K, see §1.

So the only question left is to describe the conjugacy classes in $\mathrm{PGL}_2(K)$ of the subgroups in the list. In §2 we give a general answer for subgroups of $G(K)$, for an algebraic group G, in terms of (non-abelian) Galois cohomology. We illustrate the method on one example in §3, and apply it to the case $G = \mathrm{PGL}_2$ in §4.

The motivation for looking at this question was to understand the appearance of the Brauer group in the case of $(\mathbf{Z}/2)^2$ considered in [B]. The result is somewhat disappointing, as it turns out that this case (which could be treated directly, as in [B]) is the only one where some second Galois cohomology group plays a role. At least our method explains this role, and hopefully may be useful in other situations.

Date: September 22, 2009.

1. The possible subgroups

We repeat that whenever we mention a finite group, we always assume that its order is prime to the characteristic of K. The following is classical (see [S2], 2.5).

Proposition 1.1. 1) $\mathrm{PGL}_2(K)$ *contains* $\mathbf{Z}/r$ *and* D_r[1] *if and only if* K *contains* $\zeta+\zeta^{-1}$ *for some primitive* r*-th root of unity* ζ*.*

2) $\mathrm{PGL}_2(K)$ *contains* $\mathfrak{A}_4$ *and* $\mathfrak{S}_4$ *if and only* -1 *is the sum of two squares in* K*.*

3) $\mathrm{PGL}_2(K)$ *contains* $\mathfrak{A}_5$ *if and only if* -1 *is the sum of two squares and* 5 *is a square in* K*.*

Proof : One way to prove this is to use the isomorphism $\mathrm{PGL}_2(K) \xrightarrow{\sim} \mathrm{SO}(K,q)$, where q is the quadratic form $q(x,y,z)=x^2+yz$ on K^3 ([D], II.9). If a group H embeds into $\mathrm{SO}(K,q)$, we have a faithful representation ρ of H in K^3, which preserves an indefinite quadratic form.

• Case $H=\mathbf{Z}/r$: let g be a generator; the existence of q forces the eigenvalues of $\rho(g)$ in $\overline{K}$ to be of the form $(\zeta,\zeta^{-1},1)$, with ζ a primitive r-th root of 1. This implies $\zeta+\zeta^{-1}\in K$. Conversely, if $\lambda:=\zeta+\zeta^{-1}$ is in K, the homography $z\mapsto \dfrac{(\lambda+1)z-1}{z+1}$ is an element of order r of $\mathrm{PGL}_2(K)$.

• Case $H=D_r$: by the previous case, if $D_r\subset \mathrm{PGL}_2(K)$, $\lambda:=\zeta+\zeta^{-1}$ is in K. Conversely if $\lambda\in K$, the homographies $z\mapsto 1/z$ and $z\mapsto \dfrac{(\lambda+1)z-1}{z+1}$ generate a subgroup of $\mathrm{PGL}_2(K)$ isomorphic to D_r.

• Cases $H=\mathfrak{A}_4,\mathfrak{S}_4$ or $\mathfrak{A}_5$. The representation ρ must be irreducible. Each of the groups $\mathfrak{A}_4$ and $\mathfrak{S}_4$ has exactly one irreducible 3-dimensional representation with trivial determinant, which is defined over the prime field; the only invariant quadratic form (up to a scalar) is the standard form $q_0(x,y,z)=x^2+y^2+z^2$. Thus $\mathfrak{A}_4$ and $\mathfrak{S}_4$ are contained in $\mathrm{PGL}_2(K)$ if and only if q_0 is equivalent to λq for some $\lambda\in K^*$, which means that q_0 represents 0.

Since $\mathfrak{A}_5$ contains elements of order 5, the condition $\sqrt{5}\in K$ is necessary. Suppose this is the case, and put $\varphi=\frac{1}{2}(1+\sqrt{5})$; the subgroup

[1] We denote by D_r the dihedral group with $2r$ elements.

of $\mathrm{SO}(K, q_0)$ preserving the icosahedron with vertices

$$\{(\pm 1, 0, \pm\varphi)\ ,\ (\pm\varphi, \pm 1, 0)\ ,\ (0, \pm\varphi, \pm 1)\}$$

is isomorphic to $\mathfrak{A}_5$. It follows as above that $\mathfrak{A}_5$ embeds in $\mathrm{SO}(K, q)$ if and only if q_0 represents 0. $\square$

2. Some Galois cohomology

2.1. In this section we consider an algebraic group G over K, and a subgroup $H \subset G(K)$. We choose a separable closure K_s of K, and put $\mathfrak{g} := \mathrm{Gal}(K_s/K)$. We are interested in the set of embeddings $H \hookrightarrow G(K)$ which are conjugate in $G(K_s)$ to the natural inclusion $i : H \hookrightarrow G(K)$, modulo conjugacy by an element of $G(K)$. We denote this (pointed) set by $\mathrm{Emb}_i(H, G(K))$.

We will use the standard conventions for non-abelian cohomology, as explained for instance in [S3], ch. I, §5. We will also use the notation of [S3] for Galois cohomology: if G is an algebraic group over K, we put $\mathrm{H}^i(K, G) := \mathrm{H}^i(\mathfrak{g}, G(K_s))$.

Proposition 2.2. *Let Z be the centralizer of H in $G(K_s)$. The pointed set $\mathrm{Emb}_i(H, G(K))$ is canonically isomorphic to the kernel of the natural map $\mathrm{H}^1(K, Z) \to \mathrm{H}^1(K, G)$.*

Proof : Let $X \subset G(K_s)$ be the subset of elements g such that $g^{-1}\,{}^\sigma g \in Z$ for all $\sigma \in \mathfrak{g}$. The group $G(K)$ (resp. Z) acts on X by left (resp. right) multiplication. By [S3], ch. I, 5.4, cor. 1, the kernel of $\mathrm{H}^1(K, Z) \to \mathrm{H}^1(K, G)$ is identified with the (left) quotient by $G(K)$ of the subset of $\mathfrak{g}$-invariant elements in $G(K_s)/Z$; but this subset is by definition X/Z, so we can identify our kernel to the double quotient $G(K)\backslash X/Z$.

For every $g \in X$, the conjugate embedding gig^{-1} belongs to $\mathrm{Emb}_i(H, G(K))$. Any element $j \in \mathrm{Emb}_i(H, G(K))$ is of the form gig^{-1} for some $g \in G(K_s)$; for $\sigma \in \mathfrak{g}$, the element ${}^\sigma g$ again conjugates i to j, hence $g^{-1}\,{}^\sigma g \in Z$ and $g \in X$. Thus the map $g \mapsto gig^{-1}$ from X to $\mathrm{Emb}_i(H, G(K))$ is surjective. Two elements g and g' of X give the same element in $\mathrm{Emb}_i(H, G(K))$ if and only if g' belongs to the double coset $G(K)gZ$. Therefore the above map induces a canonical bijection $G(K)\backslash X/Z \xrightarrow{\sim} \mathrm{Emb}_i(H, G(K))$. $\square$

2.3. Let us write down the correspondence explicitly: a class in our kernel is represented by a 1-cocycle $\mathfrak{g} \to Z$ which becomes a coboundary in G, hence is of the form $\sigma \mapsto g^{-1}\,{}^{\sigma}g$ for some $g \in X$; we associate to this class the embedding gig^{-1}.

2.4. We are actually more interested in the set $\mathrm{Conj}(H, G(K))$ of subgroups of $G(K)$ which are conjugate to H in $G(K_s)$, modulo conjugacy by $G(K)$. Associating to an embedding its image defines a surjective map $im : \mathrm{Emb}_i(H, G(K)) \to \mathrm{Conj}(H, G(K))$. The normalizer N of H in $G(K_s)$ acts on H by automorphisms, hence also on $\mathrm{Emb}_i(H, G(K))$. Two embeddings with the same image differ by an automorphism of H, which must be induced by an element of N if the embeddings are conjugate under $G(K_s)$. It follows that *im induces an isomorphism* $\mathrm{Emb}_i(H, G(K))/N \xrightarrow{\sim} \mathrm{Conj}(H, G(K))$.

2.5. Let us translate this in cohomological terms. Let $\mathrm{H}^1(K, Z)_0$ denote the kernel of the map $\mathrm{H}^1(K, Z) \to \mathrm{H}^1(K, G)$. An element n of N acts on $\mathrm{Emb}_i(H, G(K))$ by $j \mapsto j \circ \mathrm{int}(n^{-1})$; if $j = gig^{-1}$, this amounts to replace g by gn, hence the 1-cocycle $\varphi : \sigma \mapsto g^{-1}\,{}^{\sigma}g$ by $n^{-1}\varphi\,{}^{\sigma}n$. This formula defines an action of N on $\mathrm{H}^1(K, Z)$ which preserves $\mathrm{H}^1(K, Z)_0$; *the map $g \mapsto gHg^{-1}$ induces an isomorphism of pointed sets* $\mathrm{H}^1(K, Z)_0/N \xrightarrow{\sim} \mathrm{Conj}(H, G(K))$.

3. An example

3.1. In this section we fix an integer $r \geq 2$, prime to $\mathrm{char}(K)$, and we assume that K contains a primitive r-th root of unity ζ. We consider the matrices $A, B \in \mathrm{M}_r(K)$ defined on the canonical basis $(e_1, \ldots, e_r)$ of K^r by

$$A \cdot e_i = e_{i+1} \quad , \quad B \cdot e_i = \zeta^i e_i$$

for $1 \leq i \leq r$, with the convention $e_{r+1} = e_1$.

The matrices A and B generate the K-algebra $\mathrm{M}_r(K)$, with the relations

$$A^r = B^r = I \quad , \quad BA = \zeta AB \ .$$

Their classes $\bar{A}, \bar{B}$ in $\mathrm{PGL}_r(K)$ commute; we consider the embedding $i : (\mathbf{Z}/r)^2 \hookrightarrow \mathrm{PGL}_r(K)$ which maps the two basis vectors to $\bar{A}$ and $\bar{B}$. The image H of i is its own centralizer; in particular, H is a maximal commutative subgroup of $\mathrm{PGL}_r(K)$.

By the Kummer exact sequence (and the choice of ζ), the group $\mathrm{H}^1(K, \mathbf{Z}/r)$ is identified with K^*/K^{*r}; the pointed set $\mathrm{H}^1(K, \mathrm{PGL}_r)$ can be viewed as the set of isomorphism classes of central simple K-algebras of dimension r^2 ([S1], X.5).

Lemma 3.2. *Let $\alpha, \beta \in K^*$, and let $\bar\alpha, \bar\beta$ be their images in K^*/K^{*r}. The map $\mathrm{H}^1(i) : \mathrm{H}^1(K, \mathbf{Z}/r)^2 \to \mathrm{H}^1(K, \mathrm{PGL}_r)$ associates to $(\bar\alpha, \bar\beta)$ the class of the cyclic K-algebra $A_{\alpha,\beta}$ generated by two variables x, y with the relations $x^r = \alpha$, $y^r = \beta$, $yx = \zeta xy$.*

Proof : We choose α', β' in K_s with $\alpha'^r = \alpha$ and $\beta'^r = \beta$. The Kummer isomorphism associates to (α, β) the homomorphism $(a, b) : \mathfrak{g} \to (\mathbf{Z}/r)^2$ defined by

$$ {}^\sigma\alpha' = \zeta^{a(\sigma)}\alpha' \qquad {}^\sigma\beta' = \zeta^{b(\sigma)}\beta' \qquad \text{for each } \sigma \in \mathfrak{g} \ . $$

Its image in $\mathrm{H}^1(K, \mathrm{PGL}_r(K_s))$ is the class of the 1-cocycle $\sigma \mapsto \bar A^{a(\sigma)}\bar B^{b(\sigma)}$.

Now let us recall how we associate to the algebra $A_{\alpha,\beta}$ a cohomology class $[A_{\alpha,\beta}]$ in $\mathrm{H}^1(K, \mathrm{PGL}_r)$ (*loc. cit.*). We choose an isomorphism of K_s-algebras $u : \mathrm{M}_r(K_s) \xrightarrow{\sim} A_{\alpha,\beta} \otimes_K K_s$. For each $\sigma \in \mathfrak{g}$, $u^{-1}\,{}^\sigma u$ is an automorphism of $\mathrm{M}_r(K_s)$, hence of the form $\mathrm{int}(g_\sigma)$ for some g_σ in $\mathrm{PGL}_r(K_s)$. Then $[A_{\alpha,\beta}]$ is the class of the 1-cocycle $\sigma \mapsto g_\sigma$.

In our case we define u on the generators A, B by $u(A) = \beta' y^{-1}$, $u(B) = \alpha'^{-1}x$. Then the automorphism $u^{-1}\,{}^\sigma u$ multiplies A by $\zeta^{b(\sigma)}$ and B by $\zeta^{-a(\sigma)}$, which gives $g_\sigma = \bar A^{a(\sigma)}\bar B^{b(\sigma)}$ as above. □

3.3. The exact sequence

$$ 1 \to \mathbf{G}_m \to \mathrm{GL}_r \to \mathrm{PGL}_r \to 1 $$

gives rise to a coboundary homomorphism $\partial_r : \mathrm{H}^1(K, \mathrm{PGL}_r) \to \mathrm{H}^2(K, \mathbf{G}_m) = \mathrm{Br}(K)$ which is injective (*loc. cit.*). The class $\partial_r[A_{\alpha,\beta}] \in \mathrm{Br}(K)$ is the *symbol* $(\alpha, \beta)_r$; it depends only on the classes of α and β (mod. K^{*r}). The map $(\ ,\ )_r : (K^*/K^{*r})^2 \to \mathrm{Br}(K)$ is bilinear and alternating. Since ∂_r is injective, we find:

Proposition 3.4. *The set $\mathrm{Emb}_i((\mathbf{Z}/r)^2, \mathrm{PGL}_r(K))$ is isomorphic to the set of couples (α, β) in $(K^*/K^{*r})^2$ such that $(\alpha, \beta)_r = 0$.* □

We will describe the correspondence more explicitely in the case $r = 2$ in the next section.

4. Conjugacy classes in $\mathrm{PGL}_2(K)$

Proposition 4.1. *Assume that K is separably closed. Two finite subgroups of $\mathrm{PGL}_2(K)$ which are isomorphic (and of order prime to $\mathrm{char}(K)$) are conjugate.*

Proof : Again this is certainly well-known; we give a quick proof for completeness. The possible subgroups are those which appear in Proposition 1.1.

An element of order r of $\mathrm{PGL}_2(K)$ comes from a diagonalizable element of $\mathrm{GL}_2(K)$, hence is conjugate to the homothety $z \mapsto \zeta z$ for some $\zeta \in \boldsymbol{\mu}_r(K)$ [2]; thus a cyclic subgroup of order r of $\mathrm{PGL}_2(K)$ is conjugate to the group H_r of homotheties $z \mapsto \lambda z,\ \lambda \in \boldsymbol{\mu}_r(K)$.

There is only one group D_r containing H_r, namely the subgroup generated by H_r and the involution $z \mapsto 1/z$; it follows that all dihedral subgroups of order $2r$ are conjugate to this subgroup.

For the three remaining groups, we use again the isomorphism $\mathrm{PGL}_2(K) \xrightarrow{\sim} \mathrm{SO}_3(K)$. The groups $\mathfrak{A}_4$ and $\mathfrak{S}_4$ have exactly one irreducible representation of dimension 3 with trivial determinant, while $\mathfrak{A}_5$ has two such representations which differ by an outer automorphism: this is elementary in characteristic 0, and the general case follows by [I], ch. 15. Therefore two isomorphic subgroups H and H' of $\mathrm{SO}_3(K)$ of this type are conjugate in $\mathrm{GL}_3(K)$. The only quadratic forms preserved by H or H' are the multiple of the standard form; thus the element g of $\mathrm{GL}_3(K)$ which conjugates H to H' must satisfy ${}^t g\, g = \lambda I$ for some $\lambda \in K$. Replacing g by $\pm\mu g$, with $\mu^2 = \lambda^{-1}$, we have $g \in \mathrm{SO}_3(K)$, hence our assertion. $\square$

Recall that the determinant induces a homomorphism $\overline{\det}$: $\mathrm{PGL}_2(K) \to K^*/K^{*2}$.

Theorem 4.2. 1) $\mathrm{PGL}_2(K)$ *contains only one conjugacy class of subgroups isomorphic to $\mathbf{Z}/r$ $(r > 2)$, $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$.*

2) *The conjugacy classes of cyclic subgroups of order 2 of $\mathrm{PGL}_2(K)$ are parametrized by K^*/K^{*2}: to $\alpha \in K^*$ $(\mathrm{mod.}\, K^{*2})$ corresponds the involution $z \mapsto \alpha/z$.*

[2] As usual we denote by $\boldsymbol{\mu}_r(K)$ the group of r-th roots of unity in K.

3) *The homomorphism* $\overline{\det} : \mathrm{PGL}_2(K) \to K^*/K^{*2}$ *induces a bijective correspondence between:*

- *conjugacy classes of subgroups of* $\mathrm{PGL}_2(K)$ *isomorphic to* $(\mathbf{Z}/2)^2$*;*
- *subgroups* $G \subset K^*/K^{*2}$ *of order* ≤ 4*, such that* $(-\alpha, -\beta)_2 = 0$ *for all* α, β *in* G (see (3.3)).

4) *Assume that* $\boldsymbol{\mu}_r(K)$ *has order* r*. The conjugacy classes of subgroups* D_r *of* $\mathrm{PGL}_2(K)$ *are parametrized by* $K^*/K^{*2}\boldsymbol{\mu}_r(K)$*. The subgroup corresponding to* $\alpha \in K^*$ (mod. $K^{*2}\boldsymbol{\mu}_r(K)$) *consists of the homographies* $z \mapsto \zeta z$ *and* $z \mapsto \alpha\eta/z$*, for* $\zeta, \eta \in \boldsymbol{\mu}_r(K)$*.*

Proof : Using Proposition 4.1 we can apply the method of §3. We give the list of the subgroups of $\mathrm{PGL}_2(K_s)$ and their centralizers:

H	$\mathbf{Z}/2$	$\mathbf{Z}/r\ (r > 2)$	$\mathbf{Z}/2 \times \mathbf{Z}/2$	$D_r\ (r > 2)$	$\mathfrak{A}_4$	$\mathfrak{S}_4$	$\mathfrak{A}_5$
Z	$\mathbf{G}_m \rtimes \mathbf{Z}/2$	$\mathbf{G}_m$	$\mathbf{Z}/2 \times \mathbf{Z}/2$	$\mathbf{Z}/2$	1	1	1

In case 1), we have $\mathrm{H}^1(K, Z) = \{1\}$ (using $\mathrm{H}^1(K, \mathbf{G}_m) = \{1\}$). The result follows from (2.5).

Case 2): We apply Proposition 2.2, taking for $i(\bar{1})$ the involution $z \mapsto 1/z$. The centralizer Z is the semi-direct product of a torus $\mathbf{G}_m$ and the subgroup $\mathbf{Z}/2$ generated by the involution $\iota : z \mapsto -z$. The pointed set $\mathrm{H}^1(K, \mathbf{G}_m \rtimes \mathbf{Z}/2)$ is identified with $\mathrm{H}^1(K, \mathbf{Z}/2) \cong K^*/K^{*2}$. The map $\mathrm{H}^1(K, \mathbf{Z}/2) \to \mathrm{H}^1(K, \mathrm{PGL}_2)$ is trivial, for instance because the injection $\mathbf{Z}/2 \to \mathrm{PGL}_2$ factors through a torus $\mathbf{G}_m$. Hence the set of conjugacy classes of involutions of $\mathrm{PGL}_2(K)$ is identified with K^*/K^{*2}.

To describe the correspondence explicitely we follow (2.3). Let $\alpha \in K^*$, and let $\alpha' \in K_s^*$ such that $\alpha'^2 = \alpha$; the class of α (mod. K^{*2}) corresponds to the class of the 1-cocycle $a : \mathfrak{g} \to \mathbf{Z}/2$ given by ${}^\sigma\alpha' = (-1)^{a(\sigma)}\alpha'$. In $\mathrm{PGL}_2(K_s)$ we have $i(a(\sigma)) = g^{-1}\,{}^\sigma g$, where g is the homography $z \mapsto \alpha' z$. Thus the subgroup corresponding to α is gHg^{-1}, which is generated by the involution $z \mapsto \alpha/z$.

Case 3): Let $i : (\mathbf{Z}/2)^2 \hookrightarrow \mathrm{PGL}_2(K)$ be the embedding which maps the basis vectors e_1 and e_2 to the involutions $z \mapsto 1/z$ and $z \mapsto -z$. By Proposition 3.4 the set $\mathrm{Emb}_i((\mathbf{Z}/2)^2, \mathrm{PGL}_2(K))$ is canonically identified to the set of couples (α, β) in $(K^*/K^{*2})^2$ with $(\alpha, \beta)_2 = 0$.

Again we make the correspondence explicit following (2.3). Let $\alpha,\beta\in K^*$ with $(\alpha,\beta)_2=0$. This means that the conic $x^2-\alpha y^2-\beta z^2=0$ is isomorphic to $\mathbf{P}^1_K$, thus there exists λ,μ in K with $\lambda^2-\alpha-\beta\mu^2=0$. We choose α' and β' in K_s such that $\alpha'^2=\alpha$ and $\beta'^2=\beta$; as above we define the homomorphisms a and $b:\mathfrak{g}\to\mathbf{Z}/2$ by

$$ {}^\sigma\alpha'=(-1)^{a(\sigma)}\alpha' \quad \text{and} \quad {}^\sigma\beta'=(-1)^{b(\sigma)}\beta' \quad \text{for each } \sigma\in\mathfrak{g}\ . $$

Put $\theta:=\dfrac{\beta'\mu}{\lambda+\alpha'}=\dfrac{\lambda-\alpha'}{\beta'\mu}$; let $g\in\mathrm{PGL}_2(K_s)$ be the homography $z\mapsto\alpha'\dfrac{z-\theta}{z+\theta}$. An easy computation gives

$$ g^{-1}\,{}^\sigma g=i(a(\sigma),b(\sigma))\ . $$

Thus the embedding of $(\mathbf{Z}/2)^2$ associated to (α,β) is gig^{-1}; it maps e_1 to the homography $h_1:z\mapsto\dfrac{\lambda u-\alpha}{z-\lambda}$, and e_2 to $h_2:z\mapsto\alpha/z$. Note that $\overline{\det}(h_1)=-\beta$ and $\overline{\det}(h_2)=-\alpha$.

Now we have to take into account the action of the normalizer N of H in $\mathrm{PGL}_2(K_s)$. This is the subgroup $\mathfrak{S}_4$ generated by H and the homographies

$$ n_1:z\mapsto\frac{z+1}{z-1}\quad ,\quad n_2:z\mapsto\iota z\ , $$

where ι is a square root of -1. We apply the recipe of (2.5). Since $n_1\in\mathrm{PGL}_2(K)$, it acts on $\mathrm{H}^1(K,H)$ through its action on H, which permutes e_1 and e_2; thus it maps $(\alpha,\beta)\in(K^*/K^{*2})\times(K^*/K^{*2})$ to (β,α). The action of n_2 on H fixes e_2 and exchanges e_1 with e_1+e_2; to get the action on $\mathrm{H}^1(K,H)$ we have to multiply by the class of the cocycle $\sigma\mapsto n_2^{-1}\,{}^\sigma n_2$, that is, $\sigma\mapsto i\big((\sigma(\iota)/\iota)\,e_2\big)$. Hence n_2 acts on $\mathrm{H}^1(K,H)$ by

$$ n_2\cdot(\alpha,\beta)=(\alpha,-\alpha\beta)\ . $$

Let $G_{\alpha,\beta}$ be the subgroup of K^*/K^{*2} generated by $-\alpha$ and $-\beta$; it is the image of H by the homomorphism $\overline{\det}:\mathrm{PGL}_2(K)\to K^*/K^{*2}$. If $G_{\alpha,\beta}\cong(\mathbf{Z}/2)^2$, the orbit $N\cdot(\alpha,\beta)$ in $(K^*/K^{*2})\times(K^*/K^{*2})$ has 6 elements, which are the couples $(-x,-y)$ with $x,y\in G_{\alpha,\beta}$, $x\neq y$. If $G_{\alpha,\beta}\cong(\mathbf{Z}/2)$, the orbit has 3 elements, which are the couples $(-x,-y)$ with $x,y\in G_{\alpha,\beta}$, $(x,y)\neq(1,1)$. Finally if $G_{\alpha,\beta}$ is trivial the orbit consists only of $(-1,-1)$. Thus the conjugacy classes of subgroups

$(\mathbf{Z}/2)^2$ in $\mathrm{PGL}_2(K)$ are parametrized by the subgroups $G \subset K^*/K^{*2}$ of order ≤ 4, with the property $(-\alpha,-\beta)_2 = 0$ for each α,β in G.

Case 4): The group D_r is generated by two elements s,t with the relations $s^2 = t^r = 1$ and $sts = t^{-1}$. We choose a primitive r-th root of unity ζ and consider the embedding $i : D_r \hookrightarrow \mathrm{PGL}_2(K)$ such that $i(s)$ is the involution $z \mapsto 1/z$ and $i(t)$ the homothety $z \mapsto \zeta z$. The centralizer is $\mathbf{Z}/2$, generated by the involution $z \mapsto -z$. As in case 2) it follows that $\mathrm{Emb}_i(D_r, \mathrm{PGL}_2(K))$ is isomorphic to $\mathrm{H}^1(K, \mathbf{Z}/2)$. Also the previous argument shows that the embedding corresponding to $\alpha \in K^*$ is the conjugate of i by the homography $z \mapsto \alpha' z$, with $\alpha'^2 = \alpha$, so it maps s to $z \mapsto \alpha/z$ and t to $z \mapsto \zeta z$.

To complete the picture we have to take into account the action of the normalizer N of $i(D_r)$ in $\mathrm{PGL}_2(K_s)$. This is the subgroup D_{2r} generated by $i(s) : z \mapsto 1/z$ and the homothety $n : z \mapsto \eta z$, where $\eta \in K_s$ is a primitive $2r$-th root of unity. The action of $i(s)$ is trivial, and n acts by multiplication by the cocycle $\sigma \mapsto n^{-1}\,{}^{\sigma}n$, which corresponds to the class of η^2 in K^*/K^{*2}. Since η^2 generates $\boldsymbol{\mu}_r(K)$, the assertion 4) follows. ☐

References

[B] A. Beauville: *p-elementary subgroups of the Cremona group*. J. of Algebra **314** (2007), 553–564.

[D] J. Dieudonné: *La géométrie des groupes classiques*. Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[I] I. Isaacs: *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006.

[S1] J.-P. Serre: *Corps locaux*. Hermann, Paris, 1962.

[S2] J.-P. Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), no. 4, 259–331.

[S3] J.-P. Serre: *Galois cohomology*. Springer-Verlag, Berlin, 1997.

Laboratoire J.-A. Dieudonné, UMR 6621 du CNRS, Université de Nice, Parc Valrose, F-06108 Nice cedex 2, France

E-mail address: `arnaud.beauville@unice.fr`